UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/635,911	08/07/2003	Petri Krohn	59643.00285	7829

32294 7590 10/31/2007

SQUIRE, SANDERS & DEMPSEY L.L.P.
14TH FLOOR
8000 TOWERS CRESCENT
TYSONS CORNER, VA 22182

EXAMINER	
WILLIAMS, JEFFERY L	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
10/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/635,911	KROHN, PETRI	
	Examiner	Art Unit	
	Jeffery Williams	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 August 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 – 74* is/are pending in the application.

4a) Of the above claim(s) *46 – 59 and 62 – 71* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-45,60,61 and 72-74* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 August 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1 – 74 are pending.

Claims 46 – 59 and 62 – 71 are withdrawn from consideration.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 74 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 74 recites the term a "second-to-first node security association". This term is indefinite because the specification does not clearly define the term and such term is not common to those of ordinary skill in the art. Thus, claim 74 is rendered indefinite.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 2, 5, 6, 8, 12 – 15, 17 – 22, 45, 61, and 71 – 74 are rejected under 35 U.S.C. 102(e) as being anticipated by Aziz et al. (Aziz), "Method and Apparatus for Providing Secure Communication with a Relay in a Network", U.S. Patent 6,643,701.

Regarding claim 1, Aziz discloses:

a first node; a second node; and at least one intermediate node between said first and second nodes; wherein said first and second nodes are ~~arranged~~ configured to be in communication and said first and second nodes have a first security association and one of said at least one intermediate node and said second node have a second security association (fig. 2:210, 230); *and wherein said first security association ~~authenticates~~ is configured to authenticate said second node to said first node and said second security association ~~authenticates~~ is configured to authenticate said at least one intermediate node to said second node* (1:64-2:2; claim 3).

Regarding claim 2, Aziz discloses:

wherein at least one of said first and second security association comprise presenting at least one certificate to a respective one of said nodes for authentication (claim 3; 5:1-22).

Regarding claim 5, Aziz discloses:

wherein said at least one intermediate node inspects information sent between said first and second nodes (9:31-39).

Regarding claim 6, Aziz discloses:

wherein said at least one of intermediate nodes modifies information sent between said first and second nodes (9:31-39).

Regarding claim 8, Aziz discloses:

wherein said first node is attached to a packet switched network (Abstract).

Regarding claim 12, Aziz discloses:

wherein said first node comprises a client device (Abstract).

Regarding claim 13, Aziz discloses:

wherein at least one of said first and second security association comprises encryption (claim 3; 5:1-22).

Regarding claim 14, Aziz discloses:

wherein said one of said at least one said intermediate node is configured to pass data packets from at least one of said first node to at least one of said second

node and from at least one of said second node to at least one of said first node (fig. 2, 6).

Regarding claim 15, Aziz discloses:

wherein said at least one intermediate node is arranged in a network gateway node (fig. 2, 6; 9:31-39 – Aziz discloses the node in the form of a network gateway and thus a "node arranged in a network gateway").

Regarding claims 17 – 20, Aziz discloses:

wherein said second node is connected to said gateway node; wherein said client device comprises a computer, user equipment, mobile station, or personal digital assistant; wherein said second node comprises a serve; wherein said second node is configured to provide a service to said first node (fig. 2; col. 7).

Regarding claims 21 and 22, Aziz discloses:

wherein the first node is configured to send a first connection message to the second node; *wherein said first connection message comprises a Transmission Control Protocol connection message* (6:11-26; 7:24-67).

Regarding claim 45, Aziz discloses:

wherein said second security association is established before said first security association (5:1-22,34-41).

Regarding claim 61, Aziz discloses:

wherein said first node comprises an Secure Socket Layer Client node (fig. 2).

Regarding claims 71 – 74, they appear to comprise essentially similar limitations as are found in the above rejected claims. Claims 71 – 74 are rejected, at least, for the same reasons shown above.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 7, 9 – 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aziz.

Regarding claims 7, 10, and 11, Aziz discloses that the plurality of client nodes are wireless communication devices (i.e. cell phones - 7:4-18), however, Aziz does not explicitly state that the wireless communication devices are "attached to a wireless network". However, the notion of a wireless communication device as attached to a wireless network would have been obvious to one of ordinary skill in the art. This would

have been obvious to one of ordinary skill because it was both well known in the art for wireless devices to be attached to wireless networks and easily within the rational sensibility of one of ordinary skill to recognize that wireless communication devices communicate wirelessly ("a wireless network").

Regarding claim 9, it is rejected, at least, for the same reasons as claim 7, and furthermore because it was well known to those of ordinary skill in the art for cellular networks to operate within a GPRS standard.

Claims 3, 4, 23 – 43, and 60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aziz in view of Dierke et al. (Dierke), "The TLS Protocol", RFC 2246.

Regarding claims 3 and 4, Aziz states the use of certificates according to the SSL or TLS standard protocol. However, Aziz does not explicitly state that the certificate is a *cryptographic certificate*. Dierke however discloses that the certificates used within the TSL protocol comprise X.509 certificates (Dierke, pg. 23). It would have been obvious to recognize the teachings of Dierke within the system of Aziz, as one of ordinary skill in the art would have been motivated to operate according to the disclosed standard of TLS.

Regarding claims 23 and 24, Aziz states the use of the SSL or TLS standard protocols. However, Aziz does not explicitly state each and every technical detail of the SSL or TLS protocol. Dierke however discloses the technical details of the TLS protocol, including details regarding session establishment (Dierke, pg. 2). It would have been obvious to recognize the teachings of Dierke within the system of Aziz, as one of ordinary skill in the art would have been motivated to operate according to the disclosed standard of TLS.

Thus the combination enables:

wherein the first node is configured to send a hello message to the at least one intermediate node; wherein said hello message comprises a Secure Socket Layer protocol handshake message (Dierke, pgs. 32-36).

Regarding claims 25 – 26, the combination enables:

wherein the at least one intermediate node is configured to make a copy of at least a part of said hello message, wherein said at least one intermediate node is configured to send said hello message to the second node (4:45-59).

Regarding claim 27, it is rejected, at least, for the same reasons as claim 23 and 24. Thus, the combination enables *wherein the second node is configured to send a hello message to the said at least one intermediate node* (Dierke, pgs. 32-36).

Regarding claims 28 – 34, the combination enables:

wherein said at least one intermediate node is configured to send a handshake message to the second node in response to receiving said hello message from said second node, wherein said second node is configured to respond to said handshake message, wherein said response comprises a Secure Socket Layer protocol handshake message, wherein said handshake message sent to the second node comprises a Secure Socket Layer protocol handshake message, wherein said handshake messages are configured to create said second security association, wherein said handshake message sent by said one of said at least one intermediate node comprises a client certificate, wherein said one of said at least one intermediate node is configured to create said client certificate when requested (Dierke, pgs. 32-36).

Regarding claim 35, the combination enables:

wherein said one of said at least one intermediate node is configured to retrieve said client certificate from a storage device (Aziz, 5:1-22).

Regarding claims 36 – 38, the combination enables:

wherein said at least one intermediate node and said second node are configured to generate at least one key to encrypt information sent between said at least one node and said second node, said at least one key being used in said second security association and wherein said first node and said second node are configured to generate at least one key to encrypt information sent there between said first node and said second node, said at least one key being used in said first security association

wherein said at least one intermediate node is configured to create said at least one key only when requested (Dierke, pgs. 32-36; Aziz, 2:36-59).

Regarding claims 39 and 40, the combination enables:

wherein said at least one intermediate node is configured to retrieve said at least one key from a storage device, wherein said at least one key is configured to be dependent on a client certificate (Dierke, pgs. 32-36; Aziz, 2:36-59, 5:1-22).

Regarding claims 41 and 42, the combination enables:

wherein at least one said client certificate certifies a known node which is known to said at least one intermediate node, wherein said client certificate certifies a holder of a specified resource (Dierke, pgs. 32-36; Aziz, 2:36-59, 5:1-22; 6:12-27, 7:4-18).

Regarding claim 43, the combination does not explicitly state that a cellular telephone comprises *one of an International Mobile Station Identity telephone number and a Mobile Station Integrated Service Digital Network telephone number.* However, it was well known to those of ordinary skill in the art for a cellular telephone to comprise such a telephone number. This would have been obvious to one of ordinary skill in the art because such numbers allow cellular telephones to communicate within a network.

Regarding claim 60, the combination enables:

wherein said second security association is based on data within said hello message sent from said second node (Dierke, pgs. 32-36).

Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Aziz in view of Immonen et al. (Immonen), "Method and System for Conducting Wireless Payments", U.S. Patent Publication 2002/0077993.

Regarding claim 16, Aziz discloses a gateway that serves to translate communications between a client and server. Aziz discloses aspects related to the security of communications via the Internet, such as electronic shopping transactions performed between a mobile client (i.e. cell phone) and a merchant (i.e. e-commerce merchant) (Aziz, 1:40-63; 4:45-59; 7:4-17). Aziz does not explicitly state that the gateway can operate according to GPRS. Immonen discloses that gateways advantageously operate according to the WAP protocol, including providing support for GPRS, so as to facilitate the communications between a mobile client and a server (Immonen, par. 2-7). It would have been obvious to one of ordinary skill in the art to recognize the teachings of Immonen for a gateway operating as a GPRS support node. This would have been obvious because one of ordinary skill in the art would have been motivated to facilitate the communications between mobile clients and servers.

Claim 44 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Aziz and Dierke in view of Immonen et al. (Immonen), "Method

and System for Conducting Wireless Payments", U.S. Patent Publication 2002/0077993.

Regarding claim 44, the combination of Aziz and Dierke discloses that authenticated mobile clients may purchase or use services from servers. The combination, however, does not disclose all details specific to electronic commerce. Specifically, the combination does not explicitly state that *at least one said client certificate authorizes said second node to charge said holder of said specified resource for services used or purchased.* Immonen discloses that a client certificate authorizes said second node to charge said holder of said specified resource for services used or purchased (Immonen, par. 60). It would have been obvious to one of ordinary skill in the art to recognize the electronic commerce teachings of Immonen within the combination of Aziz and Dierke. This would have been obvious because one of ordinary skill in the art would have been motivated to incorporate in practice features of electronic commerce so as to allow a mobile client to purchase or use services.

Response to Arguments

Applicant's arguments filed 8/8/07 have been fully considered but they are not persuasive.

Applicant argues or asserts primarily that:

(i) *...dependent claims 2-4, for example, where the first and second security associations are further defined as representing at least one certificate for authentication, a cryptographic certificate, and an X.509 certificate. Hence, when taken in proper context, Aziz's first and second end-to- end secure transmission links 210 and 230 bears no structural nor functional similarity to Applicant's claimed the first and second security associations.* (Remarks, pg. 21)

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., *the first and second security associations are further defined as representing at least one certificate for authentication, a cryptographic certificate, and an X.509 certificate*) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

(ii) *... Applicant respectfully asserts that Aziz is completely silent regarding any security association that resembles the first security association configured to authenticate the second node to the first node, or the second security association configured to authenticate the at least one intermediate node to the second node, as recited in claim 1, for example.* (Remarks, pg. 21-22)

In response, the examiner respectfully points out that Aziz clearly discloses a security association *configured to authenticate the second node to the first node* and a *second security association configured to authenticate the at least one intermediate node to the second node* (Aziz, Abstract, lines 6-10).

(iii) *Further, in the rejection the Office Action cited claim 3 of Aziz, which describes the end-to-end security links as one of a secure socket layer links and transport layer security links ... there is no suggestion or description in Aziz indicating that the end-to-end secure transmissions 210 and 230 are capable of authenticating in the manners recited in Applicant's claim 1, for example.* (Remarks, pg. 22)

In response, the examiner respectfully notes that the applicant appear to argue contrary to the applicant's own disclosure wherein the applicant teaches that security associations, such as those provided via SSL, are capable of authenticating (Applicant's Specification, par. 17, line 1). At least for this reason alone, the examiner finds the applicant's argument unpersuasive.

Election/Restrictions

This application contains claims 46 – 59 and 62 – 71 drawn to an invention nonelected with traverse in the reply filed on 4/19/07. A complete reply to the final

rejection must include cancellation of nonelected claims or other appropriate action (37 CFR 1.144) See MPEP § 821.01.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

See Notice of References Cited.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

J. Williams
AU: 2137

JW

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER